The Coverage Inkwell

Emerging Coverage Issues in Intellectual Property, Privacy, and Cyber Liability

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

October 25, 2013

INTERNET COOKIES, PERSONALLY IDENTIFIABLE INFORMATION, AND THE INTERNET

In today's world of cyberspace and mass-marketing, invasion of privacy claims based on the collection and use of personally identifiable information (or, "PII") are becoming commonplace, whether such claims are alleged in connection with network security breaches, ZIP code collecting, or use of internet cookies.

In the case *In re Google, Inc. Cookie Placement Consumer Privacy Litigation*, 2013 WL 5582866 (D. Del. Oct.9, 2013), the court tackled the issue of whether PII possess any inherent value to measure its collection in terms of damages. Holding that PII, alone, has no such value, the court dismissed the complaint, holding that the alleged collection of PII, without more, did not assert an actual injury or damage. In addition, the court held that the alleged collection of PII did not violate various statutes, including the Stored Communications Act, the Computer Fraud and Abuse Act, and the California Invasion of Privacy Act.

Internet cookies are used to track an individual's activities and communications on a particular website and across the internet. They store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services as individuals surf the internet. Merchants and advertising providers, in particular, use third-party cookies to collect information to implement targeted advertising on websites. As better explained by the *Google* court:

> Third-party cookies are used by advertising companies to help create detailed profiles on individuals, including, but not limited to an individual's unique ID number, IP address, browser, screen resolution, and a history of all websites visited within the ad network by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies—that is how the tracking takes place.

Id. at *1 (citations omitted).

Plaintiffs in *Google* alleged that defendants used coding to "trick" their Safari and/or Internet Explorer (IE) browsers into accepting third-party cookies, which then allowed defendants to track browser use and implement targeted advertising on websites. *Id.* at *1-2. Plaintiffs alleged that such purported trickery constituted an invasion of privacy and violated numerous statutes. Google moved for dismissal on the ground that the allegations failed to allege an actual injury. The court agreed with Google and dismissed the case.

In order to successfully maintain an action in federal court (i.e., to have Article III standing), a plaintiff must allege "(1) an injury-in-fact ...; (2) a causal connection between the injury and the conduct complained of; and (3) that it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.* If there is no alleged injury, there is no case.

To satisfy the actual injury requirement, Plaintiffs alleged that PII has independent value and that *any* unauthorized collection and use of PII constitutes an injury. Plaintiffs cited articles contending that PII "has monetary value and is a commodity that companies trade and sell." *Id.* According to Plaintiffs, "'[t]he cash value of users' personal information can be quantified,' with web browsing histories valued at $52 per year." *Id.* Plaintiffs also argued that Google's own practice of offering "users the opportunity to join a panel which allows Google to track the websites the user visits in exchange for gifts, such as gift cards to retailers" demonstrated the value of PII. *Id.*

The court disagreed, noting that other federal district courts "have been reluctant to equate loss of PII, *without more*, to injury in fact." *Id.*(emphasis added). In *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, *6 (C.D. Cal. Apr. 28, 2011), for instance, a California federal court found that plaintiffs lack standing because they did not "explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party." *Id.* at *3. Similarly, in *Del Vecchio v. Amazon.com, Inc.*, 2011 WL 6325910, *3 (W.D. Wash. Dec. 1, 2011), a federal court held that the possibility that plaintiffs' PII would lose value as a result of its collection did not satisfy the injury-in-fact requirement to create standing.

The *Google* court concluded that more than the mere collection and use of PII is required to allege an actual injury. In *Del Vecchio v. Amazon.com, Inc.*, 2012 WL 1997697, *2 (W.D. Wash. June 1, 2012), for instance, the court found that an actual injury was alleged when plaintiffs alleged:

> the dissemination and use of personal information belonging to them, including sensitive information about their web browsing and shopping habits, purchases, and related transaction information, *combined with* their financial information such as credit and debit card information, and their mailing and billing addresses.

Id. at *3 (emphasis in *Google*). In *Claridge v. RockYou*, 785 F. Supp. 2d 855, 858-61 (N.D. Cal. 2011), which was a network security breach case that involved the loss of "email addresses, passwords, and

login credentials for social networks like MySpace and Facebook," a reluctant court expressed doubt over "plaintiff's ultimate ability to prove his damages theory," but found, for purpose of a motion to dismiss, the allegation sufficient to allege "a generalized injury in fact."

The *Google* court held that merely showing that online PII may have "some modicum of identifiable value" is insufficient to show an injury-in-fact:

> In the case at bar, the CAC details that online personal information has value to third-party companies and is a commodity that these companies trade and sell. Examining the facts alleged in the light most favorable to plaintiffs, the court concludes that, while plaintiffs have offered some evidence that the online personal information at issue has some modicum of identifiable value to an individual plaintiff, plaintiffs have not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it.

Id. at *3.

Because, in some instances, statutory violations may confer standing even in the absence of an injury-in-fact, the *Google* court also addressed whether Plaintiffs pled sufficient facts to establish invasion of privacy claims under various statutes and California's Constitution. *Id.* at *4. The limited space permitted here does not allow me to provide an analysis of the court's decision for each statute (8!). However, here are some quick observations:

The Electronic Communications Privacy Act. Also known as the "Wiretap Act," the act imposes liability on a person who "intentionally intercepts" and discloses the "*contents*" of an "electronic communication," unless "such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception...." 18 U.S.C. §§ 2520(a), 2511(1)(a), (c), 2511 (2)(d), 2510(4). "Contents" means "any information concerning the substance, purport, or meaning of that communication," i.e., it is information the user intended to communicate, such as the spoken words of a telephone call. 18 U.S.C. § 2510(8).

Plaintiffs argued that Defendants used cookies to intercept "contents" in violation of the statute. The court disagreed, noting that most of the information collected by cookies "cannot be characterized as 'contents.'" *Id.* at *4. "Specifically, 'personally identifiable information that is automatically generated by the communication' [with a website] is not 'contents' for the purposes of the Wiretap Act." *Id.* (citing cases).

In addition, the court noted that no court has characterized a URL, which is used to identify a document's physical location on the Internet, as "contents" in connection with the Wiretap Act. *Id.* at *5. Thus, the court concluded, "[e]ven if plaintiffs' browsers were 'tricked' into sending the URLs to Google, the court concludes that Google did not intercept contents as provided for by the Wiretap Act." *Id.*

California Invasion of Privacy Act. To prevail under the act, a plaintiff must show that the defendant "willfully and without the consent of all parties to the communication, or in any unauthorized manner," intercepted, used, or disclosed the "contents or meaning" of a "communication" that is "in transit." *Id.* (citing 14 Cal. Pen. Code § 631(a).)

The court found no such violation here: "[T]he court concludes that Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies. Further, plaintiffs' allegations do not demonstrate that Google intercepted any 'contents or meaning.'" *Id.* at *6.

The Stored Communications Act. Concerned that the Fourth Amendment would not protect against unlawful searches and seizures of electronic data held by third parties, such as internet service providers, the SCA was enacted to fill this perceived gap in protection. *Id.*; 18 U.S.C. §2701, *et seq.* A person is liable under the act if he or she "(1) intentionally accesses without authorization *a facility* through which an electronic communication service is provided; or (2) intentionally exceeds an authorization *to access that facility*; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system " *Id.* at *6.

Holding that an individual's computing device (such as a computer or mobile device) is not a "facility through which an electronic communications service is provided," the *Google* court held that there was no alleged violation under the statute. *Id.* at *7.

The Computer Fraud and Abuse Act. The private action component of the statute has a minimal damage threshold. 18 U.S.C. § 1030(e), (g), *see also id.*, § 1030(a)(5)(B)(1). The court held that Plaintiffs did not allege sufficient damage to satisfy this threshold. *Id.* at *8.

The California Computer Crime Law. The statute prohibits "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Pen. Code. § 502(a). Like the CFAA, the statute also has a private cause of action that requires a certain damage threshold. *Id.* at *9. The statute also requires that the perpetrator have acted "without permission," defined by courts to mean as "accessing or using a computer, computer network, or website in a manner that overcomes technical or code-based barriers." *Id.* (citing cases).

The court held that Plaintiffs did not sufficiently alleged damage or loss. *Id.* The court also held that Plaintiffs did not meet the "without permission" requirement:

> Plaintiffs allege that Safari's default settings provide an exception to the third-party cookie blocking for situations where a user submits a form to the third-party's website servers. Google exploited this exception by adding coding to ads, such that Safari believed the exception to be satisfied and that the user had submitted a form to Google. In doing so, Google exploited a standard Safari browser function. Although Google's actions may be objectionable, Google did not access plaintiffs' browsers by "overcom[ing] technical or code-based barriers." Nor did Google

> introduce a "contaminant" to "usurp the normal operation" of plaintiffs' browsers. The method of Google's exploitation of a normal function of plaintiffs' browsers is not in dispute and does not meet the requirements of the statute[.]

Id.

The California Constitution. For a claim of invasion of privacy to be brought successfully under California's Constitution, the "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Id.* at *10. Here, the court held that Plaintiffs' claims failed this requirement:

> The transfer of inputted information (which would have occurred regardless of Google's placement of cookies) does not rise to the level of a serious invasion of privacy or an egregious breach of social norms. . . . Neither is Google's subsequent association of multiple instances of plaintiffs' inputted information with other personal information to provide targeted advertising a sufficiently serious invasion of privacy.

Id. Thus, there was no claim.

The California Unfair Competition Law. As succinctly put by the court, "[a]s discussed above, plaintiffs have not articulated an injury in fact sufficient for Article III standing. Similarly, plaintiffs have not shown a loss of money or property from Google's actions sufficient to confer standing under the UCL." *Id.* at *10.

The California Consumer Legal Remedies Act. The CLRA does not apply to the sale or license of software. *Id.* at *10. Here, the court rejected Plaintiffs' arguments that Google's advertising was a "service," as defined under the statute, and not software.

"Plaintiffs' argument that Google's advertising is a 'service' and not software is unavailing, as plaintiffs' use of software browsers and the subsequent software activity is the conduct alleged to be 'unfair.' The California case law is clear that software and software activity are not covered by the CLRA." *Id.* at *11.

What does this case mean? Plaintiffs need to allege more than just the mere collection and use of personally identifiable information in order to show an actual injury. Nor are such claims sufficient to implicate liability under many statutes. Although invasion of privacy lawsuits will continue, this case provides a potential tool for analyzing exposure.

The Coverage Inkwell

Joshua A. Mooney | Counsel
1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103-7395
Direct 215.864.6345 | Fax 215.399.9613
mooneyj@whiteandwilliams.com | whiteandwilliams.com
Assistant: Dana Genovese | 215.864-6331